James E. Cecchi
CARELLA, BYRNE, CECCHI,
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Telephone: (973) 994-1700

[Additional Attorneys on Signature Page]

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

RICARDO CUBIDES and LAURA KANTHAL-CUBIDES, Individually And On Behalf Of All Others Similarly Situated,

Plaintiffs,

v.

CENTRASTATE HEALTHCARE SYSTEM, INC. and ATLANTIC HEALTH SYSTEM, INC.,

Defendants.

Case No. _____

COMPLAINT AND
DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiffs Ricardo Cubides and Laura Kanthal-Cubides ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this class action against CentraState Healthcare System, Inc. and Atlantic Health System, Inc. (together "CentraState" or the "Defendants"). Plaintiffs make the following allegations, except as to allegations specifically pertaining to Plaintiffs, upon information and belief based on, among other things, the investigation of counsel, and review of public documents.

I. NATURE OF THE ACTION

1. Medical and financial records represent the most sensitive information available concerning a person's private affairs. These records reveal intimate and personal aspects of the human condition, such as illnesses that might carry social stigma and details about substance abuse, family planning and mental health. Congress has passed legislation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in order to protect this highly confidential data, because in the wrong hands, bad actors may target and exploit the most sensitive and vulnerable populations among the public.

2. As a medical center, CentraState had obligations to safeguard this information. This lawsuit concerns CentraState's failure to carry that burden and the resulting harm to Plaintiffs and the Class. On February 10, 2023, CentraState confirmed that they had suffered a ransomware attack that disrupted its computer systems ("Data Breach"). The health system detected the attack on December 29, 2022, and waited six weeks before informing the public.

3. Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves. This includes names, addresses, Social Security numbers, dates of birth, health insurance information, and other sensitive medical records (collectively, the "Private Information") and includes personally identifiable information ("PII") and protected

health information ("PHI") as defined by HIPAA that Defendants collected and maintained.

4. As a result of CentraState's actions, Plaintiffs and the Class Members experienced damages from: (i) theft of their Private Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Private Information; (iii) loss of value of their Private Information; (iv) the amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures; (v) CentraState's retention of profits attributable to Plaintiffs' and other customers' Private Information that CentraState failed to adequately protect; (vi) economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed to; (vii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach; and (viii) overpayments of CentraState's products and/or services which Plaintiffs purchased.

II. JURISDICTION AND VENUE

5. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is well over 100, some of whom have different citizenship from Defendants. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

6. This Court has personal jurisdiction over Defendants because they are headquartered in New Jersey; the wrongful acts alleged in this Complaint were committed in New Jersey, among other venues; and Defendants have intentionally availed themselves of this jurisdiction by marketing and selling their products and services in New Jersey.

7. Venue is proper in this District under (1) 28 U.S.C. § 1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and 28

U.S.C. § 1391(d) because the transactions giving rise to Plaintiffs' claims occurred in New Jersey; and (2) 28 U.S.C. § 1391(b)(3) in that Defendants are subject to personal jurisdiction in this District.

III. PARTIES

A. Named Plaintiffs.

8. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within New Jersey. Because Defendants have exclusive but incomplete knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

9. Plaintiff Ricardo Cubides ("Plaintiff" for purposes of paragraphs 9 –13) resides in Manalapan, New Jersey. CentraState notified Plaintiff Cubides that Plaintiff's Private Information was compromised in the CentraState Data Breach by letter dated February 8, 2023.

10. As a direct and proximate result of the breach, Plaintiff Cubides has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this Data Breach; discussing the breach with Plaintiff's family; reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud; and freezing Plaintiff's credit report. This is valuable time Plaintiff Cubides otherwise could have spent on other activities.

11. Plaintiff Cubides is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

12. Plaintiff Cubides suffered actual injury from having Plaintiff's Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and

diminution in the value of Plaintiff's Private Information, a form of property that CentraState obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

13. As a result of the Data Breach, Plaintiff Cubides anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

14. Plaintiff Laura Kanthal-Cubides resides in Manalapan, New Jersey. CentraState notified Plaintiff Kanthal-Cubides that Plaintiff's Private Information was compromised in the CentraState Data Breach by letter dated February 8, 2023.

15. As a direct and proximate result of the breach, Plaintiff Kanthal-Cubides has made reasonable efforts to mitigate the impact of the breach, including, but not limited to: conducting research about this Data Breach; and discussing the breach with Plaintiff's family; and reviewing credit reports and financial account statements for any indication of actual or attempted identity theft or fraud. This is valuable time Plaintiff Kanthal-Cubides otherwise could have spent on other activities.

16. Plaintiff Kanthal-Cubides is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

17. Plaintiff Kanthal-Cubides suffered actual injury from having Plaintiff's Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Plaintiff's Private Information, a form of property that CentraState obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

18. As a result of the Data Breach, Plaintiff Kanthal-Cubides anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

B. Defendants.

19. CentraState Healthcare System, Inc. is a private, not-for-profit health organization established in 1971 with its central location in Freehold, New Jersey.

20. Atlantic Health System, Inc. is one of the largest non-profit health care networks in New Jersey. It employs 18,000 people and more than 4,800 affiliated physicians. It is headquartered in Morristown, New Jersey.

21. On October 22, 2020, officials from Atlantic Health System, Inc. announced they were acquiring a 51% stake in CentraState Healthcare System, Inc. Since that time, Atlantic Health System, Inc. has been responsible for high-level operations and allocating capital resources for CentraState.

IV. FACTUAL BACKGROUND

A. CentraState Healthcare System, Inc. is a Prominent Healthcare Provider in New Jersey.

22. CentraState, based in Freehold, New Jersey, is a private, not-for-profit health organization established in 1971 that serves New Jersey patients. CentraState includes an acute care hospital, an ambulatory campus, three senior living communities, six family practice offices, OB/GYN services, a residency training program, and a charitable foundation.

B. The Data Breach.

23. On February 10, 2023, CentraState confirmed they had suffered a ransomware attack that disrupted their computer systems. The health system detected the attack on December

29, 2022, blocked the unauthorized access, and launched an investigation to determine the nature and scope of the breach. CentraState confirmed that the hackers gained access to part of its systems. The stolen information included names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers, and patient account numbers. Complimentary credit monitoring and identity theft protection services were offered to individuals who had their Social Security number exposed.

24. Plaintiffs each received a letter dated February 8, 2023 stating *inter alia* the following:

> **What Happened?** On December 29, 2022, CentraState detected unusual activity involving our computer systems. We immediately took steps to contain the incident and initiated an investigation, which included assistance from a forensics firm. We also reported the incident to law enforcement, including the Federal Bureau of Investigation, and have been working with the FBI throughout the investigation. The investigation determined that on December 29, 2022, the unauthorized person obtained a copy of an archived database that stored patient information.
>
> **What Information Was Involved?** Our investigation determined that some of your information may have been included in the database, such as your name, address, date of birth, Social Security number, health insurance information, medical record number, patient account number, as well as information related to care that you received at CentraState, such as date(s) of service, physician name and department, treatment plan, diagnosis, visit notes, and/or prescription information. Your financial account and/or payment card information were not involved in this incident.
>
> **What We Are Doing & What You Can Do.** While, to date, CentraState is unaware of any misuse of your information, as a precaution, we are offering you a complimentary one-year membership in Experian® IdentityWork.SM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks8M is ct1mpletely free to you, and we understand that enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks8M, including instructions on how to activate your complimentary membership and information about identity protection, please see the additional information provided with this letter.
>
> We deeply regret any concern this incident may cause and want to assure you that

> we are committed to the security of - our systems, and we remain ready to provide the high-quality care that you and your family have come to expect from CentraState. Additionally, we are continually enhancing the security of our electronic systems and the data we maintain to help prevent events such as this from occurring in the future. Events of this nature are affecting an increasing number of companies in the U.S. and around the world, and federal government, law enforcement and industry experts are working in tandem to address this unlawful criminal activity.

C. Defendants Violated HIPAA's Requirements To Safeguard Data.

25. Defendants had duties to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of plan members' Personal Information.

26. Defendants are covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

27. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

28. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

29. HIPAA requires that Defendants implement appropriate safeguards for this information.

30. HIPAA requires that Defendants provide notice of a breach of unsecured protected

health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.

31. Despite these requirements, Defendants failed to comply with their duties under HIPAA and its own Privacy Practices. Indeed, Defendants failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiffs' and the Class Members' Personal Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h) Take safeguards to ensure that Defendants' business associates adequately protect protected health information;

i) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

32. Defendants failed to comply with their duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of members' Personal

Information.

D. Defendants were On Notice That Highly Valuable Personal Information Of Its Patients Could Be Breached.

33. Defendants were, or should have been, aware that they were collecting highly valuable data, for which Defendants knew, or should have known, there is an upward trend in data breaches in recent years.[1] Accordingly, Defendants were on notice of the harms that could ensue if they failed to protect patients' data.

34. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (Private Information)" so that these companies can take the necessary precautions to thwart such attacks.[2]

35. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web[3] sites making

---

[1] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 27, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

[2] Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited February 23, 2023).

[3] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last visited February 23, 2023).

the information publicly available.[4]

36. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[5]

E. Consequences of the Data Breach for Consumers.

37. Plaintiffs and Class Members have suffered actual harm and will continue to be harmed as a result of CentraState's conduct. CentraState failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. CentraState's failure to keep Plaintiffs' and Class Members' Private Information secure has severe ramifications. Given the sensitive nature of the Private Information stolen in the Data Breach – names, addresses, dates of birth, Social Security numbers, health insurance information, medical record numbers, and patient account number – hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. Class Members may be subject to blackmail from nefarious actors concerning the disclosure of their medical records. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

38. Plaintiffs' stolen Private Information may now be circulating on the dark web and it is highly valuable. Malicious actors use Private Information to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use

---

[4] *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (l last visited February 23, 2023); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited February 23, 2023).

[5] *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited February 23, 2023).

consumers' Private Information to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create synthetic identities.

39. Further, malicious actors often wait months or years to use the Private Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Private Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Plaintiffs' and Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the Private Information and identifies the victims as CentraState's current, former, or prospective customers materially increases the risk to Plaintiffs and the Class.

40. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[6] Moreover, there is often significant lag time between when a person suffers harm due to theft of their Private Information and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their Private Information obtained in the Data Breach is not used to harm them. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of CentraState's Data Breach. In other words, Plaintiffs have been harmed by the value of identity

[6] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07- 737/html/GAOREPORTS-GAO-07-737.htm (last visited May 8, 2022).

protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

41. Plaintiffs and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiffs' Private Information that was permitted without authorization by CentraState. This market value for access to Private Information can be determined by reference to both legitimate and illegitimate markets for such information.

42. In sum, Plaintiffs and Class Members were injured as follows: (i) theft of their Private Information and the resulting loss of privacy rights in that information; (ii) improper disclosure of their Private Information; (iii) loss of value of their Private Information; (iv) the lost value of access to Plaintiffs' and Class Members' Private Information permitted by CentraState; (v) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of CentraState's Data Breach; (vi) CentraState's retention of profits attributable to Plaintiffs' and Class Members' Private Information that CentraState failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (ix) overpayments to CentraState for goods and services purchased, as Plaintiffs reasonably believed a portion of the sale price would fund reasonable security measures that would protect their Private Information, which was not the case; and (x) nominal damages.

V. CLASS ACTION ALLEGATIONS

43. In accordance with Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs bring this case as a class action on behalf of a Nationwide Class and a New Jersey Subclass, defined

as follows:

Nationwide Class

All persons in the United States whose Private Information was maintained on the CentraState systems that were compromised as a result of the breach announced by CentraState on or around February 10, 2023.

New Jersey Sub-Class

New Jersey Sub-Class: All persons in the State of New Jersey whose Private Information was maintained on CentraState systems that were compromised as a result of the breach announced by CentraState on or around February 10, 2023.

44. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Classes each have more than 1,000 members. Moreover, the disposition of the claims of the Classes in a single action will provide substantial benefits to all parties and the Court.

45. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

a. Whether Defendants owed Plaintiffs and other Class Members a duty to implement and maintain reasonable security procedures and practices to protect their Private Information, and whether they breached that duty;

b. Whether Defendants continues to breach duties to Plaintiffs and other Class Members;

c. Whether Defendants' data security systems before the data breach met industry standards;

d. Whether Defendants failed to adequately respond to the data breach, including failing to investigate it diligently and promptly notify affected individuals in the most expedient time possible and without unreasonable delay;

e. Whether Plaintiffs and other Class Members' Private Information was

compromised in the data breach; and

f. Whether Plaintiffs and other Class Members are entitled to damages as a result of Defendants' conduct.

46. Plaintiffs' claims are typical of the Classes' claims. Plaintiffs suffered the same injury as Class Members—i.e., Plaintiffs' Private Information was compromised in the data breach.

47. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs has retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and his counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so. Neither Plaintiffs nor their counsel has interests that conflict with those of the proposed Classes.

48. Defendants have engaged in a common course of conduct toward Plaintiffs and other Class Members. The common issues arising from this conduct that affect Plaintiffs and other Class Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

49. A class action is the superior method for the fair and efficient adjudication of this controversy. In this regard, the Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Defendants. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties.

Defendants' records and the records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiffs' claims

50. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants have acted or refused to act on grounds that apply generally to Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class Members.

VI. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclass

51. Plaintiffs repeat and reallege the allegations contained in Sections I through V as if fully set forth herein.

52. CentraState collected sensitive Private Information from Plaintiffs and Class Members when using CentraState products and services.

53. CentraState owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Private Information in its possession from being compromised, lost, stolen, accessed or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing CentraState's security systems to ensure that Plaintiffs' and Class Members' Private Information in CentraState's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

54. CentraState's duty to use reasonable care arose from several sources, including but not limited to those described herein.

55. CentraState had common law duties to prevent foreseeable harm to Plaintiffs and the Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiffs and Class Members would be harmed by CentraState's failure to protect their Private Information because hackers routinely attempt to steal such information and use it for nefarious purposes, CentraState knew that it was more likely than not Plaintiffs and other Class Members would be harmed if it allowed such a breach.

56. CentraState's duty to use reasonable security measures also arose as a result of the special relationship that existed between CentraState, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted CentraState with their Private Information and sensitive healthcare information. CentraState alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

57. Defendants are covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

58. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the

information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

59. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

60. HIPAA requires that Defendants implement appropriate safeguards for this information.

61. CentraState's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Private Information by companies such as CentraState. Various FTC publications and data security breach orders further form the basis of CentraState's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

62. CentraState admits that they has a responsibility to protect consumer data, that it is entrusted with this data, and that they did not live up to its responsibility to protect the Private Information at issue here.

63. CentraState knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Private Information.

64. CentraState also had a duty to safeguard the Private Information of Plaintiffs and Class Members and to promptly notify them of a breach because of state laws and statutes that require CentraState to reasonably safeguard sensitive Private Information, as detailed herein.

65. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class Members could take appropriate measures to freeze or

lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by CentraState's misconduct.

66. CentraState breached the duties they owed to Plaintiffs and Class Members described above and thus was negligent. CentraState breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Private Information of Plaintiffs and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Private Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate manner that Plaintiffs' and the Class Members' Private Information in CentraState's possession had been or was reasonably believed to have been, stolen or compromised.

67. But for CentraState's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

68. CentraState's failure to take proper security measures to protect the sensitive Private Information of Plaintiffs and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiffs' and Class Members' Private Information.

69. Plaintiffs and Class Members were foreseeable victims of CentraState's inadequate data security practices, and it was also foreseeable that CentraState's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and Class Members as

described in this Complaint.

70. As a direct and proximate result of CentraState's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by CentraState; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of CentraState's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT 2

NEGLIGENCE *PER SE*

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclass

71. Plaintiffs repeat and reallege the allegations contained in Sections I through V as if fully set forth herein.

72. Defendants are covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part

164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

73. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

74. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

75. HIPAA requires that Defendants implement appropriate safeguards for this information.

76. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, also prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as CentraState of failing to use reasonable measures to protect Private Information.

77. The FTC publications and orders also form the basis of CentraState's duty.

78. CentraState violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. CentraState's conduct was particularly unreasonable given the nature and amount of Private Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as CentraState, including, specifically the damages that would result to Plaintiffs and Class Members.

79. In addition, under state data security statutes, CentraState had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

80. CentraState's violation of HIPAA and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

81. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

82. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

83. CentraState breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

84. Plaintiffs and Class Members were foreseeable victims of CentraState's violations of the HIPAA, the FTC Act, and state data security statutes. CentraState knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiffs' and Class Members' Private Information would cause damage to Plaintiffs and Class Members.

85. But for CentraState's violation of the applicable laws and regulations, Plaintiffs' and Class Members' Private Information would not have been accessed by unauthorized parties.

86. As a direct and proximate result of CentraState's negligence *per se*, Plaintiffs and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of

identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost value of access to their Private Information permitted by CentraState; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of CentraState's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT 3

UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclass

87. Plaintiffs repeat and reallege the allegations contained in Sections I through V as if fully set forth herein.

88. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by CentraState and that was ultimately stolen in the CentraState Data Breach.

89. CentraState was benefitted by the conferral upon it of the Private Information pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. CentraState understood that it was in fact so benefitted.

90. CentraState also understood and appreciated that the Private Information pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon CentraState maintaining the privacy and confidentiality of that Private Information.

91. But for CentraState's willingness and commitment to maintain its privacy and confidentiality, that Private Information would not have been transferred to and entrusted with CentraState.

92. Because of its use of Plaintiffs' and Class Members' Private Information, CentraState sold more services and products than they otherwise would have. CentraState was unjustly enriched by profiting from the additional services and products they were able to market, sell, and create to the detriment of Plaintiffs and Class Members.

93. CentraState also benefitted through its unjust conduct by retaining money that they should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

94. CentraState also benefitted through its unjust conduct in the form of the profits they gained through the use of Plaintiffs' and Class Members' Private Information.

95. It is inequitable for CentraState to retain these benefits.

96. As a result of CentraState's wrongful conduct as alleged in this Complaint (including among things its failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), CentraState has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

97. CentraState's unjust enrichment is traceable to, and resulted directly and

proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

98. It is inequitable, unfair, and unjust for CentraState to retain these wrongfully obtained benefits. CentraState's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

99. The benefit conferred upon, received, and enjoyed by CentraState was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for CentraState to retain the benefit.

100. CentraState's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiffs and Class Members other damages as described herein.

101. Plaintiffs have no adequate remedy at law.

102. CentraState is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on CentraState as a result of its wrongful conduct, including specifically: the value to CentraState of the Private Information that was stolen in the Data Breach; the profits CentraState received and is receiving from the use of that information; the amounts that CentraState overcharged Plaintiffs and Class Members for use of CentraState's products and services; and the amounts that CentraState should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT 4

DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclass

103. Plaintiffs repeat and reallege the allegations contained in Sections I through V as if fully set forth herein.

104. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

105. An actual controversy has arisen in the wake of the CentraState Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether CentraState is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information. Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Private Information stored by CentraState.

106. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

107. CentraState continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTC Act, and various state statutes;

108. CentraState continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

109. The Court also should issue corresponding prospective injunctive relief requiring CentraState to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

110. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at CentraState. The risk of another such breach is real, immediate, and substantial. If another breach at CentraState occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

111. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to CentraState if an injunction is issued. Among other things, if another massive data breach occurs at CentraState, Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to CentraState of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CentraState has a pre-existing legal obligation to employ such measures.

112. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CentraState, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

VII. CLAIMS ON BEHALF OF THE STATE SUBCLASS

COUNT 5

NEW JERSEY CONSUMER FRAUD ACT N.J.S.A. § 56:8-1, *ET SEQ.*

Plaintiffs, on behalf of the New Jersey Subclass

113. Plaintiffs re-allege and incorporate by reference preceding factual allegations found in Sections I through V as if fully set forth herein.

114. Plaintiffs and all Class members are "consumers" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1.

115. Defendants are a "person" as that term is defined by the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-1(d).

116. Defendants' conduct as alleged related to "sales," "offers for sale," or "bailment" as defined by N.J.S.A. 56:8-1.

117. Defendants advertised, offered, or sold goods or services in New Jersey and engaged in trade or commerce directly or indirectly affecting the citizens of New Jersey.

118. Defendants solicited Plaintiffs and Class Members to do business and uniformly and knowingly misrepresented that by joining, their Private Information was safe, confidential, and protected from intrusion, hacking, or theft.

119. Defendants misrepresented that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures.

120. Defendants intended to mislead Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

121. Defendants failed to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information in violation of N.J.S.A. 56:8-162, which was a direct and proximate cause of the Data Breach.

122. Defendants failed to provide notice to Plaintiffs and Class Members or otherwise comply with the notice requirements of N.J.S.A. 56:8-163.

123. Defendants' acts and omissions, as set forth evidence a lack of good faith, honesty in fact and observance of fair dealing, so as to constitute unconscionable commercial practices, in

violation of N.J.S.A. 56:8-2.

124. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiffs and Class Members are required to expend sums to protect and recover their Private Information, have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, and thereby suffered ascertainable economic loss.

125. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

A. Certification of the action as a Class Action under Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representative and their counsel of record as Class Counsel;

B. That acts alleged above be adjudged and decreed to constitute negligence and violations of the consumer protection laws of New Jersey;

C. A judgment against Defendants for the damages sustained by Plaintiffs and the Classes above, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendants engage third-party security auditors/penetration

testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

2. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

3. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

4. Ordering that Defendants segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, unauthorized third parties cannot gain access to other portions of Defendants' systems;

5. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendants conduct regular database scanning and securing checks; and

7. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiffs and Class Members prejudgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after service of this Complaint;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

IX. JURY TRIAL DEMANDED

Plaintiffs, individually and on behalf of all those similarly situated, requests a jury trial, under Federal Rule of Civil Procedure 38, on all claims so triable.

DATED: February 23, 2023

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi, Esq.
CARELLA, BYRNE, CECCHI, BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Tel.: (973) 994-1700
jcecchi@carellabyrne.com

Linda P. Nussbaum, Esq.
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
Tel: (917) 438-9189
lnussbaum@nussbaumpc.com

Christopher L. Ayers, Esq.
SEEGER WEISS LLP
55 Challenger Road 6th Floor
Ridgefield Park, NJ 07660
Tel.: (973) 639-9100
cayers@seegerweiss.com

Michael E. Criden, Esq.
CRIDEN & LOVE, P.A.
7301 SW 57th Court, Suite 515
South Miami, FL 33143
Tel.: (305) 357-9000
mcriden@cridenlove.com

Attorneys for Plaintiffs and the Proposed Class